Digital Alert Systems

White Paper

CAP Converters: A Regulatory Analysis

Our customers and partners have asked us for clarification of a number of key issues relating to where so-called “CAP converters” fall under current and expected FCC rules. We are pleased to provide the following analysis.

Introduction

So what is a “CAP converter”? These are devices that receive CAP messages and encode the content into to EAS protocol tones. These EAS protocol tones are used as a monitoring source for a legacy EAS unit that would still be left in place.

By definition, these devices are actually **uncertified CAP-to-EAS encoders**, compared to FCC-certified EAS encoder-decoders with integrated CAP functionality. This is a critical distinction between equipment that is FCC certified (Part 11 and Part 15 compliant) and equipment that is performing the same fundamental role, but does not have the required FCC certification.

This raises a number of regulatory and operational issues that have by and large been inadequately addressed by broadcast and cable industry. This analysis researches the regulatory and operational implications of uncertified CAP-to-EAS encoders.

Based on a reading of current FCC regulations, and conversations with staff at both the Federal Communications Commission and the Department of Homeland Security, we must conclude that these uncertified CAP-to-EAS encoders may pose significant compliance issues for EAS participants.

“CAP Converters” and Shortcomings in Compliance with FCC Rules

Uncertified CAP-to-EAS encoders are problematic in light of requirements and obligations established in CFR (2009) Title 47, Part 11. After discussions with FCC staff and other industry observers, we believe that the key provisions of Part 11 regulating EAS devices will remain in place, and will expand to encompass CAP functionality.

There are several specific subsections within Part 11 that call into question whether Uncertified CAP-to-EAS encoders meet the FCC’s requirements of EAS participants and vendors of EAS systems. Let’s review the specifics:

- The encoding of the EAS protocol (AFSK tones) from CAP formatted alerts clearly falls under the requirements set forth in §11.32 “EAS Encoder”. Any devices (hardware and/or software) performing the action of encoding EAS protocol fall under §11.32.
- §11.32 provides the specifications for all EAS Encoders. One problem for uncertified CAP-to-EAS encoders is that they mimic many of the key specifications of an EAS encoder, but pretend not to be subject to any required FCC certification.

Revision: 1.0 Publication: WPDAS-120

Digital Alert Systems
A division of **Monroe Electronics**
585-765-1155 | fax 585-765-9330
100 Housel Ave. | Lyndonville | NY | 14098
www.digitalalertsystems.com

- Basically this is a case of uncertified CAP-to-EAS encoders trying to have their cake and eat it too. Uncertified CAP-to-EAS encoders are mimicking the role of an EAS encoder, but circumventing the certification requirement. The certification requirement is plainly set forth in § 11.34 "Acceptability of the Equipment", under which an EAS Encoder used for generating the EAS codes and the Attention Signal **must be Certified** in accordance with the procedures specified in Part 11.

The points of these Part 11 requirements are not trivial. They are intended to assure the correct interoperability of these devices, produced by different vendors, to produce a level of assurance that this alerting system would carry out its duties in the face of a national emergency.

Several key parties have recognized this certification issue. A key FCC advisory council (the Communications, Security, Reliability and Interoperability Council, or "CSRIC") advised the Commission that uncertified CAP-to-EAS encoders should be FCC certified. In an expression of widespread industry understanding, the National Association of Broadcasters, Society of Broadcast Engineers as well as other broadcast and cable organizations filed comments with the FCC supporting the CSRIC recommendations.

Based on this discussion, we remain skeptical Uncertified CAP-to-EAS encoders will be allowed to circumvent the requirement of FCC certification. Broadcasters using Uncertified CAP-to-EAS encoders need to understand that they may be putting themselves in a risky position of using uncertified gear to perform a core EAS activity.

The next problem for Uncertified CAP-to-EAS encoders is that, while none of these devices have such certification, it is highly improbable they would be able to receive FCC certification before the September 2011 CAP compliance deadline.

CAP Converter (Uncertified EAS Encoder) Problems Meeting to FEMA's IPAWS CAP Requirements

FEMA has restarted conformance testing of CAP EAS units, and has amended some of their test parameters, and expanded others. By March 2011, FEMA hopes to have a public list of vendors that "conform" to the FEMA IPAWS requirements.

Uncertified CAP-to-EAS encoders may not be able to attain full FEMA IPAWS conformance, meaning they may not be authorized to connect with the IPAWS network to receive national or other EAS messages from that source. Among other issues, conformance testing is likely to reveal that it is very difficult – if not impossible – for an uncertified CAP-to-EAS encoder box to carry the new mandatory governor's alert. This is a very large problem that uncertified CAP-to-EAS encoders are not able to address, and could leave stations at risk of non-compliance.

All EAS/CAP units intended to connect to FEMA's CAP-based IPAWS system must undergo this conformance testing, or go through it again if they went through the earlier process. This effectively means all CAP/EAS units. Most importantly, if an EAS/CAP unit does not "conform", it will not be allowed to connect to the FEMA IPAWS system.

FEMA's conformance testing includes both the IPAWS CAP profile and the EAS-CAP Industry Implementation Guidelines. FEMA has confirmed that they will be testing CAP-to-EAS conversion strictly to the requirements specified in both the IPAWS profile and ECIG Guidelines. This will likely present a

major hurdle for both so-called CAP converter boxes (uncertified EAS encoders) and EAS units relying on outside devices for CAP processing.

The EAS-CAP implementation Guidelines adopted by FEMA specifies the CAP/EAS device must air a governor's "must carry" message so marked in accordance with FCC 11.55. A "Must Carry" message only overrides the device Originator and Event Code filtering for automatic forwarding. Messages for which the Governor's "must carry" authority is invoked are activated by the inclusion of an additional CAP "EAS-Must-Carry" parameter. This parameter will NOT translate from a CAP converter into a legacy EAS encoder/decoder. External CAP converters are not capable of handling this new FCC-required functionality.

Conclusion

If uncertified CAP-to-EAS encoders meet the specifications under § 11.32, and are intended for use in an EAS Participant site for EAS (as described under § 11.11), then they must be type Certified by the FCC as required under § 11.34. If uncertified CAP-to-EAS encoders do not meet all the specifications under 11.32, then they cannot receive FCC certification, and should not be used for EAS.

Further, if uncertified CAP-to-EAS encoders do not meet the data specifications adopted by FEMA, then they likewise should not be used in EAS.

The peril is for the broadcaster – the cost of equipment replacement and the fines for non-compliance would be theirs.